Nonlinear Quantum Mechanics Implies Polynomial-Time Solution for *NP*-Complete and #*P* Problems

Daniel S. Abrams*
Department of Physics, MIT 12-128b, Cambridge, Massachusetts 02139

Seth Lloyd†
d'Arbeloff Laboratory for Information Sciences and Technology, Department of Mechanical Engineering, MIT 3-160, Cambridge, Massachusetts 02139
(Received 27 January 1998)

If quantum states exhibit small nonlinearities during time evolution, then quantum computers can be used to solve *NP*-complete and #*P* problems in polynomial time. We provide algorithms that solve *NP*-complete and #*P* oracle problems by exploiting nonlinear quantum logic gates. Using the Weinberg model as a simple example, the explicit construction of these gates is derived from the underlying physics. Nonlinear quantum algorithms are also presented using Polchinski type nonlinearities which do not allow for superluminal communication. [S0031-9007(98)07489-4]

PACS numbers: 03.67.–a

Computers are physical devices: Like all physical systems, their behavior is determined by physical laws. This seemingly obvious statement has important implications, because as our understanding of physical phenomena expands, the theoretical limits to the power of computing machines may grow accordingly. Recently, it has been shown that quantum computers can in theory exploit quantum phenomena to perform tasks that classical computers apparently cannot, such as factoring large numbers in polynomial time [1], searching databases of size M in time $\sqrt{M}$ [2], or simulating the detailed behavior of other quantum systems in less than exponential time and space [3–5]. The realization that quantum mechanics could be used to build a fundamentally more powerful type of computing machine has led to a huge amount of recent activity in the field of quantum computation; for a review, see Ekert [6] or DiVincenzo [7].

It has been suggested [8–12] that under some circumstances the superposition principle of quantum mechanics might be violated—that is, that the time evolution of quantum systems might be (slightly) nonlinear. While there are reasons to believe that a theory of quantum gravity may involve such nonlinear time evolution, nonlinear quantum mechanics is at present hypothetical: Experiments confirm the linearity of quantum mechanics to a high degree of accuracy [13–16]. (There are, however, some questions about the interpretation of these tests due to the effects of nonlinear quantum mechanics [17]). Nonlinear quantum theories have also had theoretical difficulties [17–19]—including problems with superluminal communication—but there are nonlinear theories that do not appear to have these issues [17]. The validity of nonlinear quantum mechanics is an important question that can be settled only by further experiments and the requirements of theoretical self-consistency. However, this Letter is concerned not with the validity of a particular nonlinear theory, but instead with the implications of nonlinear quantum mechanics on the theory of computation, should quantum mechanics in fact turn out to be nonlinear at some level. In particular, we show that it is possible to exploit nonlinear time evolution so that the classes of problems *NP* and #*P* (including oracle problems) may be solved in polynomial time. An experimental question—that is, the exact linearity of quantum mechanics—could thereby determine the answer to what may have previously appeared to be a purely mathematical one. This Letter therefore establishes a new link between physical law and the theoretical power of computing machines. Moreover, because almost all hard computational problems that occur naturally (in computer science, physics, engineering, etc.) are contained within the class of #*P* oracle problems, this result could be practically important as well.

The class *NP* is the set of problems for which it is possible to verify a potential solution in polynomial time. These include all problems in the class *P* (those that can be solved in polynomial time) as well as the *NP*-complete problems, e.g., traveling salesman, satisfiability, and subgraph isomorphism, for which no known polynomial time algorithms exist. We phrase our algorithm in terms of an oracle (or "black box"), which calculates a function that maps an n bit input (between 0 and $2^n - 1$) to a single bit. With a polynomial time algorithm that determines if there exists an input value x for which $f(x) = 1$, it is easy to solve *NP*-complete problems.

A simple algorithm that solves the *NP* oracle problem can be thought of as an extension of Grover's database search algorithm [2] to a nonlinear regime. Suppose that it is possible to perform a nonlinear operation on a single qubit that has the following property: Somewhere on the unit sphere there exists a line (of not exponentially small extent) along which application of the operation causes nearby points to move apart exponentially rapidly. We can

 0031-9007/98/81(18)/3992(4)$15.00

exploit this behavior to solve *NP* problems in the following manner. Begin with an ordinary quantum computer (i.e., one that can perform the usual quantum logic operations) and place it in an equal superposition of all possible inputs. Then use the oracle (only once) to calculate $f(i)$ and obtain the state

$$\psi = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i, f(i)\rangle . \tag{1}$$

Now perform a $\pi/2$ rotation on each of the first n qubits. Each state $|i\rangle$ then maps into a superposition over all possible $|i\rangle$, with amplitude $\pm(1/\sqrt{2^n})$. In particular, each state $|i\rangle$ contributes $+(1/\sqrt{2^n})$ of its amplitude to the state $|00\cdots0\rangle$, for a total contribution of amplitude $\frac{1}{2^n}$ from each $|i\rangle$. At least $\frac{1}{2}2^n$ of these states correspond to a particular value of $f(i) = a$, and thus the state $|00\cdots0, a\rangle$ has amplitude at least $\frac{1}{2}$. A measurement on the first n qubits will therefore yield the state $|00\cdots0\rangle$ with probability at least $\frac{1}{4}$. The system will then be in the state

$$\psi = \frac{2^n}{\sqrt{2^{2n} - 2^{n+1}s + 2s^2}} |00\cdots0\rangle \otimes \left\{ \frac{2^n - s}{2^n} |0\rangle + \frac{s}{2^n} |1\rangle \right\}, \tag{2}$$

where s is the number of solutions i for which $f(i) = 1$. The last qubit now contains the necessary information; for small s, however, a measurement of the last qubit will almost always return $|0\rangle$, yielding no information. We wish to distinguish between the cases $s = 0$ and $s > 0$. This is accomplished by repeatedly applying the nonlinear operation to drive the states representing these two cases apart at an exponential rate: eventually, at a time determined by a polynomial function of the number of qubits n, the number of solutions s, and the rate of spreading, the two cases will become macroscopically distinguishable. A measurement on the last qubit will now reveal the solution. Of course, if the angular extent of the nonlinear region is small, it may be necessary to repeat the algorithm several times in order to determine the solution with high probability. In general, the algorithm will require $O((\pi/\eta)^2)$ trials, where η is the angular extent of the nonlinear region. The oracle may need to be called only once for η sufficiently large.

Problems in the class #*P* ask us to determine the exact number of solutions s. This is approximately found by counting the number of times that the nonlinear operator was applied. To determine s exactly, one proceeds with finer and finer estimates by rotating the final qubit such that the current best estimate is centered in the nonlinear region; in this way, applying the nonlinear operator separates states with s near this value so that they are distinguishable. With only a polynomial number of iterations, one determines the value s exactly.

The above algorithm has one disadvantage in that it requires exponential precision. It can be made robust against small amounts of noise by introducing a multiple qubit nonlinearity, as follows. Use the previous algorithm but calculate the value $f(i)$ a total of M times to obtain the state

$$\frac{2^n - s}{2^n} |000\cdots0\rangle + \frac{s}{2^n} |111\cdots1\rangle . \tag{3}$$

plus noise. By making M sufficiently large—a constant multiple of n will suffice—the amplitude of the states with more 1's than 0's (such as $|111011\ldots\rangle$) caused by random noise will be exponentially smaller than the amplitude caused by the existence of a single solution for which $f(i) = 1$. Hence, any nonlinear operator that rapidly increases the amplitude of such states with respect to the amplitude of states with more 0's than 1's will suffice to distinguish reliably the cases $s = 0$ and $s = 1$, as required. Moreover, a nonlinearity of this type satisfies the Polchinksi criterion [17] for nonlinear quantum mechanics without superluminal communication, and need not violate the second law of thermodynamics. (A similar nonlinear operator is described in more detail by Czachor in [20].)

Finally, we describe below another algorithm that is robust against small errors and show explicitly how to construct the necessary nonlinearities from the underlying physics using the Weinberg model, because of its simplicity and generality, and because it is well known. We begin as before with a quantum computer that can perform the usual quantum logic operations, and that can in addition perform a simple nonlinear operator whose form will be described shortly. In order to simplify the description, we assume for now that there is at most a single value x for which $f(x) = 1$. Once again, we begin by placing the computer in an equal superposition of all possible inputs and use the oracle (only once) to calculate $f(i)$, thereby obtaining the same state as before [Eq. (1)]. In what follows, we call the first n qubits index bits and the final qubit containing $f(i)$ the flag bit. Now consider the first (index) qubit separately, and group all the states of the superposition into pairs based on the value of qubits $2, \ldots, n$. That is, the qubits $2, \ldots, n$ define 2^{n-1} subspaces of dimension $4 = 2$ (dimensions for qubit 1) $\times$ 2 (dimensions for the flag qubit). Within each subspace, the computer will be in one of the following states (where we write the value of the first qubit followed by the value of the flag qubit, and ignore the normalization constants):

$$|00\rangle + |11\rangle , \tag{4a}$$

$$|01\rangle + |10\rangle , \tag{4b}$$

$$|00\rangle + |10\rangle . \tag{4c}$$

(At the start of the computation, most of the superposition will be in the third state, because the flag qubit is $|1\rangle$ in at most only 1 of the 2^n components.) A distinctly nonlinear transformation "N" is then applied to these two qubits (we show below how virtually any deterministic nonlinear operator can be recast into this form):

$$|00\rangle + |11\rangle \longrightarrow |01\rangle + |11\rangle, \tag{5a}$$

$$|01\rangle + |10\rangle \longrightarrow |01\rangle + |11\rangle, \tag{5b}$$

$$|00\rangle + |10\rangle \longrightarrow |00\rangle + |10\rangle. \tag{5c}$$

This transformation is like an AND gate—it ignores the index qubit and places the flag qubit in the state $|1\rangle$ if and only if either of the original components had the state $|1\rangle$ for the flag qubit [21]. The step is then repeated using each of the first n qubits as the index (and the remaining $n-1$ qubits to define the 2^{n-1} subspaces). After each iteration, the number of components in the superposition that have a $|1\rangle$ for the flag qubit doubles. After n iterations, the flag qubit is no longer entangled with the first n qubits: It is either in the state $|1\rangle$ for every component of the superposition or the state $|0\rangle$ for every component of the superposition. One can then simply measure the flag qubit to determine the solution.

Thus, if one can perform the two qubit nonlinear transformation N one can find the answer to an NP-complete problem with certainty in polynomial (in fact linear) time, using only a single evaluation of the oracle. Although the operation N may appear unnatural, it can be obtained by using ordinary unitary operations and much simpler and more "natural" single qubit nonlinear operators (that is, to the extent that any nonlinear operation in quantum mechanics can be considered "natural"). One possible technique for generating the transformation would be to use the following steps: first, act on the two qubits with the unitary operator

$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ 1 & 0 & 0 & -1 \end{bmatrix}, \tag{6}$$

where the basis is assumed to be $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$, in that order. Next, operate on the second qubit with a simple one qubit nonlinear gate $\hat{n}_-$ that maps both $|0\rangle$ and $|1\rangle$ to the state $|0\rangle$. One then obtains the state $|00\rangle$ for both cases (a) and (b), and some unknown state $|A\rangle$ for case (c) [see Eqs. (4) and (5)]. (The state $|A\rangle$ is unknown because we have not specified the behavior of the nonlinear gate on $|0\rangle + |1\rangle$ or $|1\rangle - |0\rangle$). Whatever the state $|A\rangle$ may be, we can perform a unitary operation that will transform the first qubit into the pure state $|0\rangle$ while leaving the state $|00\rangle$ in place. A second nonlinear gate $\hat{n}_+$ is now required that will map the state $x|0\rangle + y|1\rangle$ to the state $|1\rangle$, while leaving the state $|0\rangle$ unchanged. After this gate is applied, the computer is then in the state $|00\rangle$ for cases (a) and (b) and in the state $|01\rangle$ for case (c). The two qubit transformation N is then easily obtained with a NOT gate on the second qubit and a $\pi/2$ rotation on the first qubit.

Having thus shown how to generate N, the question is now reduced to that of generating the simpler single qubit gates $\hat{n}_-$ and $\hat{n}_+$. If one considers the state of a qubit as a point on the unit sphere, then all unitary operations correspond to rotations of the sphere; and while such rotations can place two state vectors in any particular position on the sphere, they can never change the angle between two state vectors. A nonlinear transformation corresponds to a stretching of the sphere, which will in general modify this angle. The desired gates $\hat{n}_-$ and $\hat{n}_+$ are two particular examples of such operations. Excepting perhaps certain pathological cases (e.g., discontinuous transformations), it is evident that virtually any nonlinear operator, when used repeatedly in combination with ordinary unitary transformations (which can be used to place the two state vectors in an arbitrary position on the sphere), can be used to arbitrarily increase or decrease the angle between two states, as needed to generate the gates $\hat{n}_-$ and $\hat{n}_+$. We describe in detail how these gates can be obtained using the model of nonlinear quantum mechanics put forth by Weinberg.

In Weinberg's model, the "Hamiltonian" is a real homogeneous nonbilinear function $h(\psi, \psi^*)$ of degree one, that is [9]

$$\psi_k \frac{\partial h}{\partial \psi_k} = \psi_k^* \frac{\partial h}{\partial \psi_k^*} = h \tag{7}$$

and state vectors time-evolve according to the equation

$$\frac{\partial \psi_k}{\partial t} = -i \frac{\partial h}{\partial \psi_k^*}. \tag{8}$$

Following Weinberg [9], one can always perform a canonical homogeneous transformation such that a two-state system (i.e., a qubit) can be described by a Hamiltonian function

$$h = n\overline{h}(a), \tag{9}$$

where

$$n = |\psi_1|^2 + |\psi_2|^2, \tag{10}$$

$$a = \frac{|\psi_2|^2}{n}. \tag{11}$$

It is easy to verify his solution to the time dependent nonlinear Schrödinger equation (8), which is

$$\psi_k(t) = c_k e^{-i\omega_k(a)t}, \tag{12}$$

where

$$\omega_1(a) = \overline{h}(a) - a\overline{h}'(a), \tag{13}$$

$$\omega_2(a) = \overline{h}(a) + (1-a)\overline{h}'(a). \tag{14}$$

For nonlinear $\overline{h}(a)$, one sees that the frequencies depend on the magnitude of the initial amplitude in each basis state. Intuitively, one can imagine a transformation on the unit sphere which, instead of rotating the sphere at a particular rate, twists the sphere in such a way so that each point rotates at a rate which depends upon its angle θ from the axis (clearly, this transformation involves stretching of the surface). One can exploit this stretching of the sphere to build the gate $\hat{n}_-$ as follows:

Step 1.—Perform a rotation on the first qubit by an angle $\phi < 45°$:

$$|0\rangle \longrightarrow \cos(\phi)|0\rangle - \sin(\phi)|1\rangle, \quad (15)$$

$$|1\rangle \longrightarrow \sin(\phi)|0\rangle + \cos(\phi)|1\rangle. \quad (16)$$

Step 2.—Time-evolve the system according to the nonlinear Hamiltonian $h = n\overline{h}(a)$. Thus

$$|0\rangle \longrightarrow \cos(\phi)|0\rangle - \sin(\phi)|1\rangle \longrightarrow \alpha\cos(\phi)|0\rangle - \beta\sin(\phi)|1\rangle, \quad (17)$$

$$|1\rangle \longrightarrow \sin(\phi)|0\rangle + \cos(\phi)|1\rangle \longrightarrow \gamma\cos(\phi)|0\rangle + \delta\sin(\phi)|1\rangle, \quad (18)$$

where α, β, γ, and δ are phase factors. Because the initial amplitudes of the basis states are different in the two cases, the nonlinear Hamiltonian will cause the components to evolve at different frequencies. As long as these frequencies are incommensurate, there is a time t at which $\alpha = \gamma = \delta = 1$ and $\beta = -1$ (to within an accuracy ε). (Further, this time t is a polynomial function of the desired accuracy ε.) The net result of these two steps is then

$$|0\rangle \longrightarrow \cos(\phi)|0\rangle + \sin(\phi)|1\rangle, \quad (19)$$

$$|1\rangle \longrightarrow \sin(\phi)|0\rangle + \cos(\phi)|1\rangle. \quad (20)$$

Step 3.—Reverse the first step. Thus

$$|0\rangle \longrightarrow \cos(2\phi)|0\rangle + \sin(2\phi)|1\rangle, \quad (21)$$

$$|1\rangle \longrightarrow |1\rangle. \quad (22)$$

Essentially, we have reduced the angle between the two states by an amount 2ϕ. By suitable repetition of this procedure (that is, by choosing ϕ appropriately for each iteration), or simply by choosing ϕ precisely in the first step, the states $|0\rangle$ and $|1\rangle$ can be mapped to within ε of the state $|0\rangle$, in an amount of time which is a polynomial function of the desired accuracy. This is the desired behavior for the nonlinear gate $\hat{n}_-$. The procedure can be modified slightly to increase the angle between state vectors and produce the desired behavior for the gate $\hat{n}_+$. We have thus shown explicitly how to solve *NP*-complete problems using the Weinberg model, using an algorithm which did not require exponentially precise operations.

To solve the problems in the class #*P*, one replaces the flag qubit with a string of $\log_2 n$ qubits and modifies the algorithm slightly—so that it adds the number of solutions in each iteration rather than performing what is effectively a one bit AND. In this case, a measurement of the final result reveals the exact number of solutions.

In conclusion, we have demonstrated that nonlinear time evolution can in fact be exploited to allow a quantum computer to solve *NP*-complete and #*P* problems in polynomial time. We have shown how to accomplish this exponential speedup using both the Polchinski and Weinberg models of nonlinear quantum mechanics. Finally, we would like to note that we believe that quantum mechanics is in all likelihood exactly linear, and that the above conclusions might be viewed most profitably as further evidence that this is indeed the case. Nevertheless, the theoretical implications and practical applications that would result from a discovery to the contrary may warrant further investigation into the matter.

D. S. A. acknowledges support from NDSEG, and helpful discussions with J. Jacobson, I. Singer, S. Johnson, I. Park, and T. Wang. Portions of this research were supported by the ONR, by ARO and DARPA under QUIC, the Quantum Information and Computation initiative, and by a DARPA grant to NMRQC, the Nuclear Magnetic Resonance Quantum Computing initiative.

*Email address: abrams@mit.edu
†Email address: slloyd@mit.edu

[1] P. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, edited by S. Goldwasser (IEEE Computer Society, Los Alamos, CA, 1994), p. 124.
[2] L. K. Grover, in *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, 1996* (ACM, New York, 1996), pp. x+661, 212–219.
[3] R. P. Feynman, Int. J. Theor. Phys. **21**, 467 (1982).
[4] S. Lloyd, Science **273**, 1073 (1996).
[5] D. S. Abrams and S. Lloyd, Phys. Rev. Lett. **79**, 2586 (1997).
[6] A. Ekert and R. Jozsa, Rev. Mod. Phys. **68**, 733 (1996).
[7] D. P. DiVincenzo, Science **270**, 255 (1995).
[8] S. Weinberg, Phys. Rev. Lett. **62**, 485 (1989).
[9] S. Weinberg, Ann. Phys. (N.Y.) **194**, 336 (1989).
[10] D. I. Fivel, Phys. Rev. A **56**, 146–156 (1997).
[11] B. G. Levy, Phys. Today **42**, No. 10, 20 (1989).
[12] O. Bertolami, Phys. Lett. A **154**, 225–229 (1991).
[13] P. K. Majumder *et al.*, Phys. Rev. Lett. **65**, 2931 (1990).
[14] R. L. Walsworth *et al.*, Phys. Rev. Lett. **64**, 2599 (1990).
[15] T. E. Chupp and R. J. Hoare, Phys. Rev. Lett. **64**, 2261 (1990).
[16] J. J. Bollinger, D. J. Heinzen, W. M. Itano, S. L. Gilbert, and D. J. Wineland, Phys. Rev. Lett. **63**, 1031 (1989).
[17] J. Polchinski, Phys. Rev. Lett. **66**, 397 (1991).
[18] A. Peres, Phys. Rev. Lett. **63**, 1114 (1989).
[19] N. Gisin, Phys. Lett. A **113**, 1 (1990).
[20] M. Czachor, quant-ph/9802051.
[21] There is one subtlety regarding nonlinear quantum mechanics which we should address here. When the superposition principle is abandoned, it is not immediately clear how entangled qubits will evolve. We follow the Weinberg model, in which the time evolution for a joint system composed of two subsystems is specified in terms of a preferred basis of vectors for the tensor product Hilbert space. For the purpose of using the nonlinear dynamics to perform quantum logic, we specify the joint dynamics in terms of the basis $\{|b\rangle\} = \{|0\cdots00\rangle, |0\cdots01\rangle, \ldots, |1\cdots11\rangle\}$ for each subsystem. The Weinberg prescription is as follows: write the joint state for the system $|\Psi\rangle_{12}$ as $\sum_b \alpha_b |b\rangle_1 |\psi_b\rangle_2$ and then act on each $|\psi_b\rangle_2$ independently with the nonlinear transformation N.